PCT ORLD INTELLECTUAL PROPERTY ORGANIZA
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06K 9/00

A2

(11) International Publication Number: WO 98/11501

(43) International Publication Date: 19 March 1998 (19.03.98)

(21) International Application Number: PCT/US97/16092

(22) International Filing Date: 10 September 1997 (10.09.97)

(30) Priority Data:

60/025,949	11 September 1996 (11.09.96)	US
08/925,524	8 September 1997 (08.09.97)	US

(71)(72) Applicants and Inventors: RAO, D., Ramesh, K. [GB/US]; 357 - 6th Avenue #5, Menlo Park, CA 94025 (US). SUBBIAH, Subramanian [IN/US]; 1326 Spruce Street #2306, Philadelphia, PA 19107 (US). LI, Yang [CN/US]; 2065 California Street #7, Mountain View, CA 94040 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: CHU, Donna [US/US]; 1326 Spruce Street #2308, Philadelphia, PA 19107 (US).

(74) Agents: HICKMAN, Paul, L. et al.; Hickman Beyer & Weaver, LLP, P.O. Box 61059, Palo Alto, CA 94306 (US).

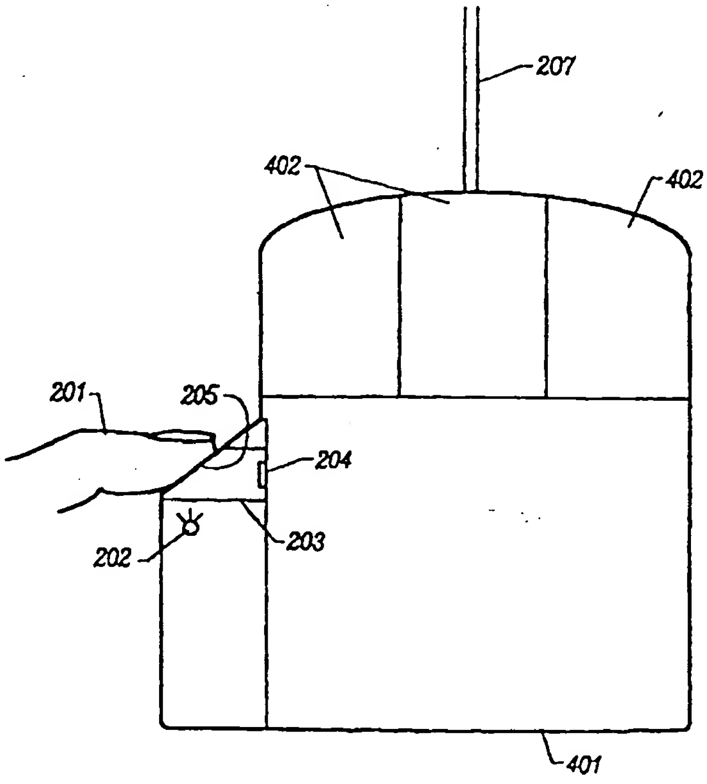
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: EMBEDDABLE MODULE FOR FINGERPRINT CAPTURE AND MATCHING

(57) Abstract

Disclosed is a low-cost fingerprint capture device that can be integrated in a computer mouse. Fingerprint information captured with such a device is transmitted to a computer via a serial port. As such ports are relatively slow, the capture device provides a low resolution fingerprint image (having less than 512 x 512 pixels). This low resolution data is processed by an iterative method that contrasts sectors of the image in a direction specified by "flow vectors". These flow vectors specify an average direction of fingerprint ridgelines in the sector under consideration. These methodologies enable the transmission of fingerprint data over the relatively slow RS232 serial protocol, in a manner that allows virtually instantaneous fingerprint identification.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Embeddable Module for Fingerprint Capture and Matching.

Cross Reference to Related Applications

This application claims priority from US Provisional Patent Application No. 60/025,949, filed September 11, 1996, entitled EMBEDDABLE MODULE FOR FINGERPRINT CAPTURE AND MATCHING, and naming R. Rao, S. Subbiah, Y. Li, and D. Chu as inventors. That application is incorporated herein by reference in its entirety and for all purposes.

Background of the Invention

This invention relates to fingerprint recognition methods and apparatus. More particularly, the invention relates to authentication systems that capture fingerprints, transmit fingerprint data through simple serial ports such as RS232 ports, and perform authentication in real time based upon the fingerprint data transmitted through the serial ports.

Today, security is a prime issue of computer networking and computing in general. In the age of global connectivity and internet information exchange, authentication and or authorization of users is essential for the protection of both users and servers. The requirement for security includes the protection of sensitive personal files on a shared computer system, protection of personal information such as credit card numbers through the Internet for purchasing/protection, etc.

Various encryption methods exist for dealing with such problems. See for example, U.S. Pat. No. 5,373,559 (Kaufman et. al.). Most of these methods involve either passwords which are often difficult for users to remember or easy for computer hackers to crack, or some more complicated algorithms that in many cases require users to carry a "calculator" that would generate a new key at each time entry to a system is desired.

In many cases, it would be preferable to use biometric information, in particular fingerprints, for security purposes, since these are unique, do not require memorization on the part of the user, and are difficult to duplicate. Fingerprint technology including hardware image capture, software image processing, software/hardware for fingerprint data storage and software for fingerprint analysis/comparison is a relatively mature technology with over 20 years of prior art methodology (See for example, U.S. Patents Nos. 2,952,181, 4,151,512, 4,322,163, 4,537,484, 4,747,147, and 5,467,403). It is well-known that no two individuals possess the identical fingerprint and that accurate matching techniques in conjunction with well-captured images can positively identify an individual.

Hardware for fingerprint capture and software algorithms for subsequent fingerprint searching, matching, authentication and verification are available from many vendors for high-security purposes (e.g. from Identix of Sunnyvale, California; Digital Biometrics of Minnentonka, Minnesota; Printrack of Los Angeles, California; Morpho of France), and are routinely used by the police and more recently by other governmental entities for, e.g., verifying the identity of social welfare recipients and motorists registering with the Department of Motor Vehicles. The complete hardware/software systems require sizable investments, ranging from a few thousand dollars to many tens of thousands of dollars (larger more sophisticated systems can run into millions). The hardware capture devices are generally bulky -- approximately the size of a standard brick -- and need to be attached to a computer via an additional board that usually connects to the system bus. These boards are usually full-size or half-size boards of at least four inches by four inches and have to be specially installed within the computer housing and peripheral interface.

At present, a low cost (consumer market pricing of significantly less than 100 dollars), miniaturized (about the size of the finger itself), and easily usable fingerprint-based protection of user identity, privacy, and computer data - particularly for internet commercial applications - is not available for the general home/individual consumer/personal computer owner. The lack of such a low-cost, extremely small, and readily usable fingerprint-based security device is a significant constraint that prevents widespread everyday use of fingerprints.

Summary of the Invention

The present invention provides a low-cost fingerprint capture device that can be integrated in or totally embedded within various existing computer peripherals. Fingerprint information captured with such a device may be used for authorization to use computer systems, for encryption of computer files and directories, for authorization/authentication when accessing remote computer stations/peripheral equipment including those connected by the internet/world wide web, and for general verification/authentication of the identity of the user. The hardware computer peripherals suitable for such integration include various types of existing mouse, glidepads, trackballs, keyboards, and other related mechanisms where a user controls access or inputs data to a computer.

Since many of these peripherals communicate with the computer through serial ports or relatively slow parallel ports, the transmission of the captured fingerprint information is a bottleneck to real-time (i.e. instantaneous, under a second) fingerprint verification. The present invention introduces advanced methodologies which enable the transmission of such information, in particular over the slow RS232 serial protocol, in a manner that allows virtually instantaneous fingerprint identification.

One aspect of the invention provides an apparatus for identifying a user's fingerprint. This system may be characterized as including the following features: (a) a fingerprint capture module which generates an image of the user's fingerprint in a low resolution format comprised of fewer than 512 x 512 pixels (thereby allowing rapid transmission over the RS232 format); (b) a connection line connected to the fingerprint capture module and capable of transmitting the low resolution fingerprint image; and (c) a processor connected to the connection line and configured to determine relative positions of minutiae in the low resolution fingerprint image.

To generate the low resolution fingerprint image, the fingerprint capture module preferably includes a CCD array, a CMOS photodiode/photogate array, an imaging capacitor array formed on a semiconductor substrate, or an imaging ultrasonic mechanism. The low resolution fingerprint image preferably comprises at most 240 x 240 pixels, more preferably at most 160 x 240 pixels, and most preferably at most 160 x 120 pixels. To ensure real time fingerprint processing, the connection line preferably transmits such low resolution fingerprint image in not more than about two seconds.

Another aspect of the invention provides a method of identifying a user's fingerprint. This method may be characterized as including the following: (a) obtaining an image of a fingerprint; (b) generating a plurality of "flow vectors" from the fingerprint image; (c) contrasting the fingerprint image using the flow vectors to generate a flow contrasted fingerprint image; and (d) extracting fingerprint minutiae from the flow contrasted fingerprint image. Each of the flow vectors specifies an average direction of ridgeline flow at a sector in the image. Preferably, the method also "thins" the flow contrasted fingerprint image prior to extracting the fingerprint minutiae.

Often steps (b) and (c) are repeated until the flow contrasted fingerprint image converges. In such an iterative procedure, a step of thinning the flow contrasted fingerprint image may be performed in each iteration.

These and other features and advantages of the invention will be described in detail below with reference to the associated figures.

Brief Description of the Drawings

Figure 1A is a table listing some of the signals transmitted on various pins of an RS232 connector

Figure 1B is an illustration depicting the connections for two serial ports communicating according to the RS232 format.

Figure 1C is a timing waveform illustrating transmission of signals according to the RS232 format.

Figure 1D is an illustration depicting the pin arrangement on an RS232 connector.

Figure 2A is a side sectional view of a fingerprint capture module in accordance with one embodiment of the present invention.

Figure 2B is a top sectional view of the fingerprint capture module shown in Figure 2A.

Figure 3 is a side sectional view of optics that may be employed in one embodiment of a fingerprint capture module of this invention.

Figure 4A is a top view of a computer mouse outfitted with a side mount fingerprint capture module suitable for use with this invention.

Figure 4B is a top view of a computer mouse outfitted with an internal mount fingerprint capture module suitable for use with this invention.

Figure 5 is a flow-diagram representative of a conventional process employed in fingerprint processing software.

Figure 6 is a thinned image of a low resolution (160 x 120 pixel) fingerprint image and processed by conventional fingerprint recognition software such that the thinned image has an unacceptably high number of false fusions.

Figure 7 is a flow diagram depicting a fingerprint minutiae extraction technique that may be employed with low resolution fingerprint images of the present invention.

Figure 8 is an illustration comparing thinned images derived from high and low resolution images of a fingerprint.

Detailed Description of the Preferred Embodiments

For purposes of this discussion, the term "computer" will generically refer to all computing devices, including personal computers, network computers, bridges, routers, work stations, supercomputers, embedded computer processor chips, etc.

The term "fingerprint" as used herein refers to handprints, palmprints, and other unique skin patterns in addition to traditional fingerprints.

For convenience, most of the peripherals discussed herein will be referred to generically as "generic computer mouse" or simply "mouse." These include, for example, various types of existing mouse, glidepads, trackballs, keyboards, and other related mechanisms where a user controls access or inputs data to a computer.

The discussion below will present certain preferred apparatuses and methodologies for implementing the present invention. First, certain information setting forth preferred environments of the invention will be described. These include serial ports (particularly those adhering to the RS232 format) and computer processing of conventional fingerprint data. It should be understood that many details discussed herein are provided simply to help illustrate the invention and are not necessarily intended to limit the invention. Thus, the invention may be practiced without limitation to some or all of the details set forth to illustrate preferred embodiments.

It should be understood that the present invention also relates to machine readable media on which are stored software produced in accordance with the requirements of this invention, or program instructions for performing methods of this invention. Such media include, by way of example, magnetic disks, magnetic tape, optically readable media such as CD ROMs, semiconductor memory such as PCMCIA cards, etc. In each case, the medium may take the form of a portable item such as a small disk, diskette, cassette, etc., or it may take the form of a relatively larger or immobile item such as a hard disk drive or RAM provided in a computer. Furthermore, program instructions implementing this invention may sometimes be transported over a communications network.

A. Serial Ports

As known in the state of the art, there are two types of standard ports on computers, including personal computers, that are used to communicate data with peripheral components: one is the parallel type of port which uses eight separate lines to transmit data in parallel, and the other is the serial type of port/interface which uses a single line. As they are physically larger, and occupy more external surface area, there is typically only one parallel port available on a computer. Serial ports, however, are smaller'and often more than one is present on a computer. Serial ports come in a variety of formats of which the most common is the standard RS232 type that was developed in the early days of telephone communication.

Another type of serial port that is common on a computer is the PS/2 serial port which is originally developed by IBM Corporation of Armonk, NY. Today, some computers, particularly personal computers that are IBM-compatible, have them.

The higher-capacity parallel port is typically used by printers, some scanners, digital cameras, and other peripheral components that deliver large quantities of information to the computer. The lower capacity serial ports are typically used by less data-intensive computer control/data input peripherals of the "generic mouse" and telephone modems. In particular, on IBM-compatible personal computers, the PS/2 type of serial port is solely dedicated to service the computer mouse and keyboard. On many IBM-compatible personal computers a computer mouse can be attached through either the PS/2 serial port or alternatively through additionally available RS232 serial ports. On non-IBM-compatible personal computers, any of the available RS232 ports can be used by the computer mouse.

With the serial port interface, where the RS232 data transmission format is virtually a de-facto standard, the constraints of efficiently transmitting fingerprint information requires special consideration that the present invention overcomes. Even when a faster transmission format is employed, the present invention allows fingerprint recognition to be performed in a manner that consumes less computer resources.

Figures 1a to 1d illustrate the RS232 serial communication protocol established by the Institute of Electronic and Electrical Engineers (IEEE) as an international standard for telephone communication. As known in the state of the art, the standard allows for specific pin numbers 101 (Figure 1a) on an RS232 connector 106

(Figure 1d) to correspond to electrical wires attached to it that specifically carry out the many different functions 112 (Figure 1a) required for efficient communication between two devices 111 using the RS232 serial protocol. The wires are of two broad types -- control lines and those that are specifically used to transmit data, like fingerprint image data. For example pin number 2 (102) carries information transmitted in one direction 108 while pin number 4 (104) requests the data to be sent, and pin number 7 (107) is the signal ground.

Figure 1b illustrates how some of these electrical wires are physically attached to either end of the serial communication link 111. For instance, the signal ground 110 of the connectors at either end are wired together while the electrical line for transmitted data 105 from the transmitting connector is wired to the electrical line for received data on the receiving connector 109 and vice versa.

Figure 1c illustrates the actual scheme for packaging the bits of information to be sent/received using the transmit 102 or receive 103 electrical lines. As is explained in detail on pg. 477 of Horowitz and Hill (The Art of Electronics. 1980, Cambridge University Press), hereby incorporated by reference for all purposes, anywhere between 4 to 8 data bits can be sent in a single packet which can be additionally framed by one start bit and one stop bit. The packets can be transmitted at various allowed baud rates (bits per second) that ascend as follows -- 110, 150, 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, 115,200. Typically, even the latest personal computers do not allow for sustained RS232 serial transmission rates higher than 115,200 baud.

B. Reducing the Quantity of Transmitted Fingerprint Image Data

When higher rates of data transmission are required by a peripheral, the data has to be transmitted directly to the bus through either a special bus port or more commonly through a dedicated board that has to be inserted into a computer. Fingerprint image data which is highly voluminous, is currently sent through a dedicated board that connects directly to the bus.

The present invention alleviates the inconvenience that users of captured fingerprint information face when forced to install a dedicated computer board/card onto the mother board bus itself. One embodiment of the present invention is directed to the use of the external parallel port (without a special card) for obtaining captured fingerprint information from a computer peripheral.

Conventionally, the RS232 serial ports and even slower PS/2 ports are not used for fingerprint recognition because the maximum rate of serial data that can be handled by present-day computers (typically using the 16550 UART chip which is well known is the state of the art) is only 115,200 bits per second (baud rate). The time required to send a fingerprint image that is not specially processed for the RS232 standard (i.e., not employing the techniques of the present invention) is in the few tens of seconds at the maximum baud rate presently available. While the parallel port is typically several time faster than the serial port, the required time is still more than a few seconds -- at least without the special processing that the present invention provides.

Even if the faster parallel port is used, fingerprint capture peripherals provided through such parallel port would not be the ideal solution. Note that a typical personal computer has only one parallel port and many competing peripherals like printers, scanner etc. to occupy it. Often no such competition exists for serial ports; frequently there is at least one spare RS232 serial port available. The present invention has the advantage of being suitable for use with an external serial port, in particular those which use the slow but common RS232 serial format, to transmit captured fingerprint information.

Still further, the present invention provides the use of the low-capacity RS232 format itself to deliver the voluminous data normally associated with the fingerprint images. Because the physical data transfer-rate is slow, the present invention preferably employs special handling (described below) of the fingerprint data to accommodate the RS232 format and sends the information very rapidly (typically on the order of a second or two).

Such efficient use of the slow RS232 format is facilitated by a biometric processing routine that we have developed. For real-time instantaneous fingerprint-matching, the RS232 protocol is too slow to transmit fingerprint images at a resolution sufficiently high for image processing by traditional fingerprint software. In order to achieve rapid transmission over RS232 serial lines the current invention allows capture of a relatively coarse and significantly low-resolution fingerprint image. This limits the amount of data that must be transmitted over the serial port. It also limits the quantity of processing resources that must be deployed to process the fingerprint data. Thus, fingerprint recognition can be performed in real time even when the fingerprint is captured on a device connected by a relatively slow serial port.

In prior recognition systems such advantages were not attainable because far higher resolution data was required to perform accurate fingerprint matching. In the present invention, the transmitted fingerprint image may be rather crude in comparison to that typically processed by prior art algorithms (see for U.S. Pat. No. 2,952,181, 4,151,512, 4,322,163, 4,537,484, 4,747,147, 5,467,403 and NIST manuals). Thus, an important aspect of the current invention is a methodology that we have developed to overcome the crudeness of the transmitted fingerprint data and restore higher resolution features of the original fingerprint. In effect the lower resolution of the transmitted print, while allowing rapid transmission, introduces ambiguities in the details of the fingerprint image, that prior art methods cannot restore. Since these details are crucial to subsequent accurate fingerprint comparison, the current invention, unlike the prior art, provides a special methodology (described below) for correctly resolving these ambiguities prior to traditional fingerprint comparison. Therefore, the methods of this invention allow for the rapid and efficient use of the RS232 serial protocol, whose speed was heretofore inadequate, to transmit captured fingerprint information and allow real-time fingerprint comparison.

At the currently available maximum baud rates (which represents the bulk of the installed base of computers well into the next century) of 115,200 bits per second, the transmission of the standard resolution fingerprint data is much too slow. The 'Federal Bureau of Investigation (FBI) and National Institute of Standards (NIST) approved' fingerprint images require 512 x 512 = 262,144 individual pixels each with 256 levels of gray shades (represented by 8 bits), would take some (262 144 x 8)/ 115,200 = 18.2 seconds. This is hardly real-time and is unacceptable for the envisaged swift and interactive consumer uses that low-cost fingerprint technology can be widely put to.

For fingerprint technology to take-off with average consumers, fingerprint image transmission should occur on the order of one second. The present invention achieves such a real-time transmission on standard RS232 lines by two means, one hardware and the other software. Further, it is the particular marriage of these two means that allows this rapid transmission possible. First, lower resolution and therefore coarser fingerprint images - in one embodiment 240 x 160 = 38 400 pixels and in a further preferred embodiment only 160 x 120 = 19 200 pixels - are transmitted over the RS232 serial line. This can be done by using CCD or CMOS photodiode/photogate cameras with suitably lower number of pixels. However, cameras with such non-standard pixel numbers are relatively expensive compared with the standard ones mass produced for the multimedia/video market like 512 x 512 and 320 x 240 pixels. Therefore one aspect of our invention requires the adaptation of these higher-resolution cameras to only send alternate lines of pixels and within these lines only every other pixel. In general, the invention applies to any technology in which an image of lower resolution than the standard 512 x 512 pixel image (i.e., an image containing less than 262,144 pixels) is transmitted from a computer peripheral for further processing.

Suitable hardware logic circuitry allows the 512 x 512 camera to send only 240 x 240 pixels and the 320 x 240 camera to send only 160 x 120 pixels. In another embodiment, the 320 x 240 camera can be arranged to only send out one contiguous half of the pixels, so that the camera window is now half at 160 x 240 pixels. In a further embodiment only every other row of the 320 rows is dropped to give a different type of camera window that is also 160 x 240. However, a preferred embodiment adapts the 320 x 240 camera for use as the really coarse 160 x 120 camera mentioned above.

Another aspect of this data reduction whereby higher resolution fingerprint data is dropped in favor of quicker transmission of fingerprint images is the adoption of gray levels that are coarser than the standard 256 shades. In one preferred embodiment, the system employs a coarser 64 gray scale that can be encoded in 6 bits, in combination with the lower number of pixel results in complete but less detailed fingerprint images that can be contained in as little as 160 x 120 x 6 = 115,200 bits of data. Such relatively crude images can be transmitted on a RS232 line operating at 115,200 baud in about 1 second (see Figures 1a-1d for further details; see also pg. 477-78 of Horowitz and Hill, The Art of Electronics. 1980, Cambridge University Press)

While the real-time (about 1 second) constraint for fingerprint data transmission can now be met, the crudeness of the images causes problems in interpreting and analyzing these fingerprint images received by the computer. In particular, a 160 x 120 image is at or even beyond the theoretical limit required for preserving the unique patterns of fingerprint ridgelines that define and so differentiate one human being from another.

A typical human fingerprint has a aspect ratio of 3 to 2 (i.e., it is 1/2 time as long as it is wide). The average fingerprint has about 50 to 60 ridgelines separated by intervening valleylines that are about equally as thick. Generally the lines run from left to right and as they do they first traverse upwards and later downwards. Even if these lines were horizontal and did not traverse longitudinally, and each ridgeline was one pixel thick and each valleyline was also one pixel thick, one would need at least 60 x 2 = 120 pixels in the longitudinal direction to clearly resolve all the lines. This is the reason for the FBI-approved choice of 512 x 512 pixels since it allows for at least four pixels per ridgeline and four per valleyline. With the stringent choice of 160 pixels, as in a preferred embodiment, allowing for the generally curved and non-horizontal ridgelines would still be pushing the limit for resolving truly independent ridgelines as being separate. That is to say one will inadvertently generate many fusions between ridgelines that are spurious.

C. Structure of a Fingerprint Capture Module

Figures 2A and 2B show, respectively, side and top views of an exemplary arrangement of components on a fingerprint image capturing module 200. Finger 201 is pressed on the surface 205 of the optical mount 203 which sits on top of an image capturing device such as a CCD camera 204 (or a CMOS photodiode/photogate camera). There is a light source 202 that uniformly illuminates the finger 201. The light source 202 could be a single LED which is part of a larger diffuser that would provides uniform lighting over the entire finger 201 at the surface 205. The circuit board 206 is preferably smaller than a one or two square inches in area. The cable 207 extends from the circuit board 206 to the RS232 serial communication port. For clarity, electronic components, other than CCD 204, on the circuit board 206 are not shown. Such other components include, for example, RS232 drivers, analog-to-digital converters, power supplies, clocks, FPGA controllers, and timers.

Figure 3. illustrates the details of an exemplary optical and lighting apparatus. Lighting source 202 could be a single LED which can be powered from the circuit board 206. The optical mount 203, which securely fits over the CCD 204, is enlarged and shown in detail. It can be made from a single molded piece of acrylic material. The lens 301 is shown to be part of the optical mount 203. The surface 205 is where the user presses his/her finger 201. The optical mount 203 allows light to travel from the illuminated finger 201 to the CCD camera 204.

In an alternative embodiment, the fingerprint capture module may be an imaging capacitor array formed on a semiconductor substrate such as that described in the May 22, 1997 edition of the San Francisco Chronicle, "New Chip Verifies Fingerprints" which pertains to a product of Veridicom Corporation. An advantage of this embodiment is that it does not require the optics for focusing an image of the fingerprint onto the CCD or CMOS array. In another alternative embodiment, imager 417 may be an ultrasonic mechanism formed on semiconductor substrates.

Figures 4A and 4B shows two exemplary embodiments of a fingerprint capturing device that can be integrated/embedded into a generic or common computer mouse 401. The generic mouse 401 has the typical components of a mouse such as mouse button(s) 402. The cable 207 to the RS232 serial port can transmit the data from both the mouse 401 and the circuit board 206 of the fingerprint capturing device that is embedded in the mouse 401. The particular embodiment shown in Figure 4B only requires a small opening to be carved from the side of the mouse where finger 201 could be pressed onto the surface 205 of the optical mount 203. The embodiment shown in Figure 4A requires the molding of the common mouse 401 to be slightly enlarged on one side. This embodiment is intended to fit the shape of a hand comfortably. Although not shown, this fingerprint capturing device/module can be integrated easily into other serial peripheral components such as glidepads, trackballs, and keyboards.

In a further refinement of the present invention, the fingerprint module itself can include an on-board embedded computer processing chip that can at least partly process the captured fingerprint image locally. Such partly processed fingerprint information from a fingerprint capture peripheral can be sent for further processing/interpretation to either another computer typically larger connected to it or other electronic peripherals using the same RS232 serial telephony format itself. Therefore, the present invention also provides the use of the RS232 format for transmitting partly processed fingerprint information captured by the fingerprint capture device between computers (including embedded computers on-board the fingerprint capture device itself) and all peripheral equipment connected to them by such a RS232 serial format. In some embodiments, the capture module uniquely identifies the fingerprint by extracting minutiae (described below), while the processing module matches the newly captured fingerprint against one or more stored fingerprints.

It should be understood that while many benefits of the invention can be realized when implemented on a peripheral connected over a serial port, the invention can also be deployed in devices connected to parallel ports.

D. Minutiae Extraction from High Resolution Fingerprints

Accurate fingerprint matching technology, which is well-known in the art (see, for example, U.S. Patent Nos. 2,952,181, 4,151,512, 4,322,163, 4,537,484, 4,747,147, and 5,467,403 which were previously incorporated by reference), has for over a hundred years relied on the extraction and subsequent comparison of specialized features called minutiae. Minutiae are essentially of two equally frequent types - either the abrupt ending of a line in the middle of the fingerprint or the fusion of two lines to create a Y-shaped junction. Typically there are about 60 or 70 such features in a fingerprint and it is the relative location of these from each other that creates a unique spatial pattern that statistically no other human can possess.

Traditional methods of fingerprint matching may involve software processing steps as illustrated in Figure 5. After capturing the fingerprint image (step 501) with an FBI-standard 512 x 512 pixel array, a contrasting step (step 503) reduces all the gray shades of a captured image 502 to either black (for ridgelines) or white (for valley lines) as shown in image 504. Traditionally these methods are omni-directional. That is, *a priori*, they have no notion of what direction the ridge lines are generally flowing at any given pixel. Basically, the particular shade of gray at each pixel is compared with those of the neighboring pixels in all directions and if judged to be relatively darker than most of its neighbors it is deemed to be black, otherwise white. For the purpose of contrasting the present invention from traditional methodology, a key point is that the judgment in traditional methods is made without any knowledge of the general direction of the overall ridge-flow in the fingerprint.

After this contrasting step, the contrasted image 504 is further processed by a thinning method (step 505). The object here is to reduce the black lines from being on average four pixels thick to only one pixel thick, thereby increasing the number of white pixels substantially. A thinned image 506 is then examined by further methods (step 507) that attempt to deduce and accurately extract the minutiae and their locations as shown in a map 508. The process is then completed at 509. All further fingerprint matching/comparison relies only on these 60 or 70 extracted pieces of information. Therefore the generation of false minutiae is particularly damaging to their use as a means to uniquely identify individuals.

When the high-resolution 512 x 512 captured image 502 as shown in Figure 5 is processed by traditional software as described, a nice separation between ridgelines 803 (Figure 8) results in extraction of only true minutiae/features 508 and 804.

Figure 6 provides an example of a low resolution 160 x 120 pixel fingerprint image that was image processed using the procedure of Figure 5. Remember that the procedure of Figure 5 is meant to apply to higher-resolution 512 x 512 images without benefit of the methods of this invention. Referring directly to Figure 6, note the extremely large number of false contacts/fusions between independent ridgelines, that thereby swamping the smaller number of real minutiae.

Owing to the lack of resolution, when the traditional method (Figure 5) is routinely applied to a coarse 160 x 120 pixel image, the thinned image can be typically expected to look like a tangled mass with numerous false fusions overwhelming the true ones. This is to be compared with the nicely thinned image 506 in Figure 5. Thus, reducing the resolution in order to send less pixel in the 1-second rather than the 18-second time-frame down a RS232 serial line will traditionally result in a set of fingerprint minutiae that is so corrupted that it is worthless for the purpose of fingerprint-based identification of individuals. Thus, a mass market for fingerprint technology based on exploiting the widely installed RS232 serial line route (e.g. mouse or keyboard) appears untenable.

E. Extracting Minutiae from Low Resolution Fingerprints

Figure 7 is a modification of the traditional fingerprint image processing schemes illustrated in Figure 5 that includes two methodologies to allow coarser 160 x 120 images to be used to extract accurate minutiae without introducing false minutiae that may arise due to the low-resolution. In particular, a directional contrasting method 703 and a flow-vector generating method 705 are used in a cyclical manner until nicely resolved thinned images (like those from 512 x 512 images) are obtained even from 160 x 120 images.

Together these methods allow the artificially generated false minutiae stemming from the coarse 160 x 120 images to be detected and removed, leaving only the true minutiae (i.e. ridgeline fusions). In an initial cycle, the modified method proceeds as usual from the captured image 701, to an omnidirectional contrasting step 702, and to a thinning step 704. Then a new method step 705 calculates general flow vectors over an entire thinned image 710. In a preferred embodiment, step 706 is performed as follows. The thinned image is divided into relatively course square sectors and a general preferred average direction of the ridgeline flow is computed for each sector. These flow vectors are then temporarily stored.

It has been found that this method works well if the fingerprint image is divided into at least about 100 sectors. Even better results can sometimes be obtained if the image is divided into between about 300 and 500 sectors (400 sectors in a particularly preferred embodiment). Depending upon the number of pixels in the image array, each sector may include between about fifteen by fifteen pixels and thirty by thirty pixels, for example.

In one embodiment, the flow vectors in each sector are generated as follows. Each pixel in the sector is analyzed to generate its own flow vector. Then, the flow vectors for each pixel in the sector are averaged to obtain a sector flow vector. Note that each pixel's flow vector simply comprises a direction of arbitrary but uniform magnitude. Therefore, to obtain a sector's flow vector, the directions of all pixel flow vectors within the sector are linearlly averaged. The flow vector for a given pixel may be obtained as follows. The pixels surrounding the pixel under consideration are each considered to determine which of them contain "ink" and which do not. From this, a direction of the ink can be obtained, and that direction defines the flow vector for the pixel under consideration. In one approach, only those pixels in the two nearest rings surrounding the pixel under consideration are considered in generating the local flow vector.

Unlike traditional methods, this method does not immediately proceed to minutiae/feature extraction (step 708). Rather, it cycles through directional contrasting (step 703), thinning (step 704), and flow vector generation (step 705) until the flow vectors converge. Each time, the original captured image (provided in step 701) is contrasted with the newly generated flow vectors. Only on the initial cycle is omnidirectional contrasting (step 702) performed.

Each time the new flow vectors are generated, the system compares the newly generated set of flow vectors against the set of flow vectors from the previous cycle at a step 706. Alternatively, step 706 could be performed by comparing the newly thinned image against the thinned image from the previous cycle. If the thinned image is improving (as determined at decision step 706), process control is directed to a step 703 where a novel contrasting method turns the gray shaded image into a black/white one in a directional manner. At each pixel, the local general ridgeline flow vector that was previously temporarily stored for the vicinity of a sector under consideration is used to selectively darken or lighten pixels in that direction. Instead of using neighboring pixels in all directions as a baseline for assessing the darkness or lightness of the pixel, pixels along the ridge flow vector direction as well as pixels along a direction completely orthogonal to it are used to make the judg,nent. This directionally contrasted image is then thinned as normal at step 704. Again the new ridge flow vectors are calculated over all sectors at step 705. If the thinned image appears to be improving 706, the entire cycle of directional contrasting 703, thinning 704 and flow vector generation 705 is repeated until convergence as determined at step 706.

One approach to specifying convergence is as follows. All flow vectors from the current iteration are compared against those from the immediately previous iteration. If the average change in flow vector direction (averaged over all sectors of the image) is less than a defined amount (5° for example), then the procedure is deemed to have converged. In an alternative embodiment, if the average change in flow vector direction is less than the average standard deviation (average over the standard deviations for each sectors), the image is deemed to have converged. Note that the standard deviation for a given sector is obtained by considering the local flow vectors for all pixels making up that sector.

When the method finally determines at step 706 that the image has converged, process control is directed to a step 708 where the minutiae are extracted. The procedure is then completed at a step 709. The net result of this procedure is a thinned image of even 160 x 120 pixel coarse images that are substantially free of artefactual false fusions stemming from the lack of sufficient resolution in the captured image.

This process of removal of false fusions is illustrated in more detail in Figure 8. In a portion of a 512 x 512 fingerprint image 802, well separated ridges are obtained. The one true Y-shaped fusion 804 is clearly found correctly in the thinned image where the thinned lines 803 are nicely resolved. When the same portion of the same fingerprint is captured at the lower 160 x 120 image resolution 806, one can clearly see the ill-effects of the use of coarser pixels - ridgelines that are so close to each other that any two parallel lines inadvertently touch each other at many points along their lengths. When this coarser image is thinned by traditional methods, these spurious points of contact lead to multiple false fusions that swamp the one real fusion in a relatively useless thinned image 807. Nevertheless, when instead the above method is applied (indicated by arrow 808) to the coarser 160 x 120 image 803, it is possible to obtain the well-resolved thinned images, showing the only one true fusion 804, characteristic of the higher-resolution 512 x 512 image.

After the minutiae have been extracted, they are typically matched against the stored fingerprints. This requires matching the two-dimensional coordinates of the stored and recently captured fingerprints. If the coordinates match to within a defined tolerance, the tokens are deemed a match.

As known in the state of the art, many fingerprint matching schemes involve the generation of inter-minutiae-based keys (i.e., distance vectors, etc.) that while being generally similar, will vary between multiple impressions of the same finger. Various inter-minutiae distance-vector-derived formats are known in the art. Many of these (as well as variations on them) may be suitable for use with this invention.

Suitable matching schemes are described in, for example, US Patent No. 4,747,147 issued to Sparrow on May 24, 1988, US Patent No. 5,493,621 issued to Matsumura on February 20, 1996, and information provided at the World Wide Web site www.Lucent.Com/Press/0597/minu1.GAF. Each of these documents is incorporated herein by reference for all purposes. A typical description of a processed fingerprint is a list of x, y and angle tabulation of each minutia. Minor modification to these linear values (e.g., adding slight random displacements) will still reflect the same underlying fingerprint, allowing for variation during multiple impressions (e.g., slight distortions and rolling during the pressing of the finger).

In conclusion the introduction of the above-described method allows coarse fingerprint images, that would be normally useless in the context of prior art minutiae extraction methods, to be nevertheless of use for fingerprint recognition. This ability to use such low-resolution data enables exploitation of the slow but overwhelmingly common RS232 serial line to deliver real-time fingerprint comparison to the mass consumer market.

F. Other Embodiments

In general, the present invention provides techniques which allow rapid processing of fingerprint images to extract minutiae with relatively little expenditure of computational resources. Such techniques may be deployed in numerous applications. For example, they may allow comparison of stored fingerprint data with a user's fingerprint data taken at the time of installation or operation of a software program. Such methods may be employed for the purpose of controlling software distribution. Various methodologies employing such comparison may be used in this invention. Some of these methodologies are described in US Patent Application Serial No. 08/___,___ (Attorney Docket No. HUSHP002), entitled A BIOMETRIC BASED METHOD FOR SOFTWARE DISTRIBUTION, naming S. Subbiah, D. R. K. Rao, and Y. Li as inventors, and filed on the same day as the instant patent application. That application is incorporated by reference for all purposes.

Another potential use of such a system involves giving the software manufacturer the option of charging its clients by usage -- either by usage time or number of users. That is, the concept of pay-per-use. If the original user or buyer is given the option of adding additional users by the program, then the program can keep track of the number of users and the amount of elapsed time at each use. Such information can be sent back to the manufacturer periodically, either by postal mail for the first method or electronic mail for the second method, for billing purposes.

In another embodiment, this invention is employed in a system and method employing a user's fingerprint to authenticate a wireless communication. The user's personal fingerprint is employed as the secret key in the context of a modified "challenge-response" scenario. The system includes a fingerprint capture module on a mobile personal wireless communication device (e.g., a wireless telephone) and a central authentication system coupled to a conventional mobile switching center. The central authentication system contains information that associates each mobile identification number ("MIN") with a particular user's fingerprint. When a wireless communication is to be initiated, the central authentication system engages in a challenge-response authentication with the mobile switching station or the wireless phone using the stored fingerprint associated with the MIN through the common air interface. The correct response from the mobile station will only be generated when the user's fingerprint entered through the fingerprint capture module attached to the mobile station matches the information sent from the central authentication system, and only calls placed from authorized users are connected. This embodiment is described in US Patent Application Serial No. 08/___,___ (Attorney Docket No. HUSHP003), entitled METHOD OF USING FINGERPRINTS TO AUTHENTICATE WIRELESS COMMUNICATIONS, naming Y. Li, D. R. K. Rao, and S. Subbiah as inventors, and filed on the same day as the instant patent application. That application is incorporated by reference for all purposes.

While this invention has been described in terms of a few preferred embodiments, it should not be limited to the specifics presented above. Therefore, the invention should be broadly interpreted with reference to the following claims.

CLAIMS

What is claimed is:

1. An apparatus for identifying a user's fingerprint, the system comprising:

a fingerprint capture module which generates an image of the user's fingerprint in a format comprised of fewer than 512 x 512 pixels;

a connection line connected to the fingerprint capture module and capable of transmitting the fingerprint image in the format comprised of fewer than 512 x 512 pixels; and

a processor connected to the connection line and configured to determine relative positions of minutiae in the fingerprint image.

2. The apparatus of claim 1, wherein the fingerprint capture module includes a CCD array or a CMOS photodiode/photogate array.

3. The apparatus of claim 1, wherein the fingerprint capture module includes an imaging capacitor array formed on a semiconductor substrate or an ultrasonic mechanism formed on a semiconductor substrate.

4. The apparatus of claim 1, wherein the fingerprint capture module provides the fingerprint image in a format comprising 240 x 240 pixels.

5. The apparatus of claim 1, wherein the fingerprint capture module provides the fingerprint image in a format comprising 160 x 240 pixels.

6. The apparatus of claim 1, wherein the fingerprint capture module provides the fingerprint image in a format comprising 160 x 120 pixels.

7. The apparatus of claim 1, wherein the connection line is capable of transmitting the fingerprint image in not more than about two seconds.

8. The apparatus of claim 1, wherein the connection line transmits the fingerprint image in the RS232 format.

9. The apparatus of claim 1, wherein the processor is provided in a computer and the fingerprint capture module is provided in a computer peripheral.

10. The apparatus of claim 9, wherein the computer peripheral is a mouse, a trackball, a keyboard, or a glidepad.

11. The apparatus of claim 1, wherein the processor is provided in a cellular telephone.

12. The apparatus of claim 1, wherein the processor contrasts and thins the fingerprint image prior to determining the relative positions of the minutiae in the user's fingerprint.

13. The apparatus of claim 1, wherein the processor contrasts the fingerprint image with a plurality of flow vectors from the fingerprint image, each of the flow vectors specifying an average direction of ridgeline flow at a sector in the image.

14. A method of identifying a user's fingerprint, the method comprising:

(a) obtaining an image of a fingerprint;

(b) generating a plurality of flow vectors from the fingerprint image, each of the flow vectors specifying an average direction of ridgeline flow at a sector in the image;

(c) contrasting the fingerprint image using the flow vectors to generate a flow contrasted fingerprint image; and

(d) extracting fingerprint minutiae from the flow contrasted fingerprint image.

15. The method of claim 14, further comprising:

thinning the flow contrasted fingerprint image prior to extracting the fingerprint minutiae.

16. The method of claim 14, wherein (b) and (c) are repeated until the flow contrasted fingerprint image converges.

17. The method of claim 16, further comprising a step of thinning the flow contrasted fingerprint image generated in each iteration.

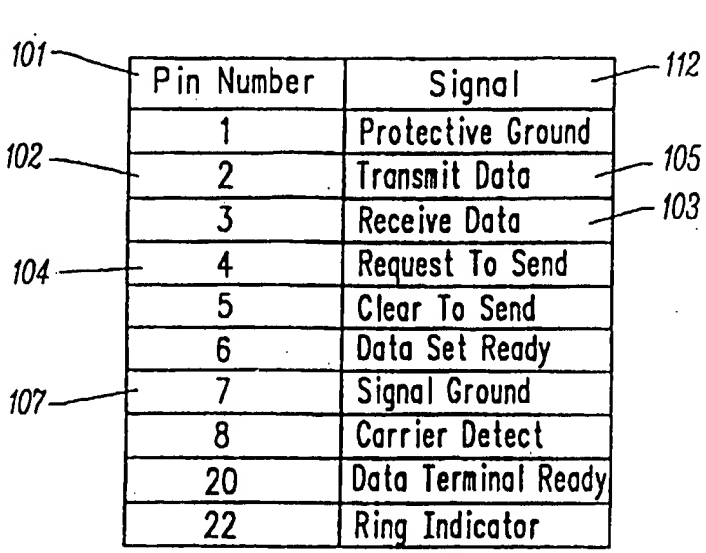
18. The method of claim 16, wherein the fingerprint image is provided in a format comprising 240 x 240 pixels.

19. The method of claim 16, wherein the fingerprint image is provided in a format comprising 160 x 240 pixels.

20. The method of claim 16, wherein the fingerprint image is provided in a format comprising 160 x 120 pixels.

21. The method of claim 16, wherein the fingerprint image is provided from a computer peripheral over a connection line that transmits the fingerprint image in an RS232 format.

22. The method of claim 21, wherein the computer peripheral is a mouse, a trackball, a keyboard, or a glidepad.


101
102
104
107
112
105
103

Pin Number	Signal
1	Protective Ground
2	Transmit Data
3	Receive Data
4	Request To Send
5	Clear To Send
6	Data Set Ready
7	Signal Ground
8	Carrier Detect
20	Data Terminal Ready
22	Ring Indicator

FIG. 1A

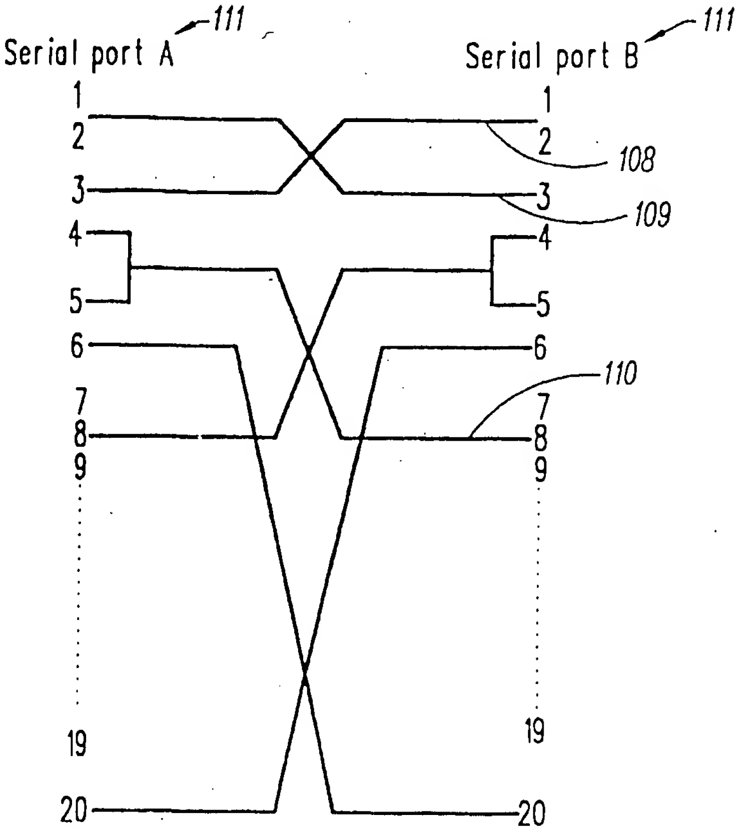


FIG. 1B

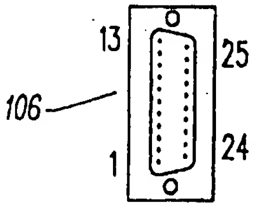


FIG. 1D

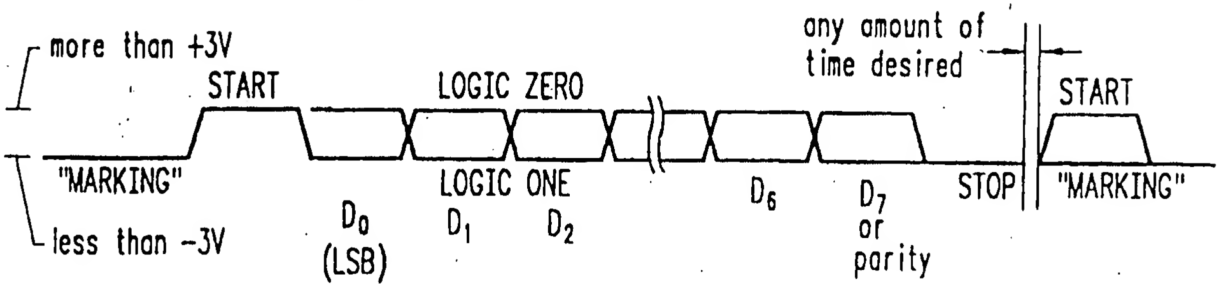


FIG. 1C

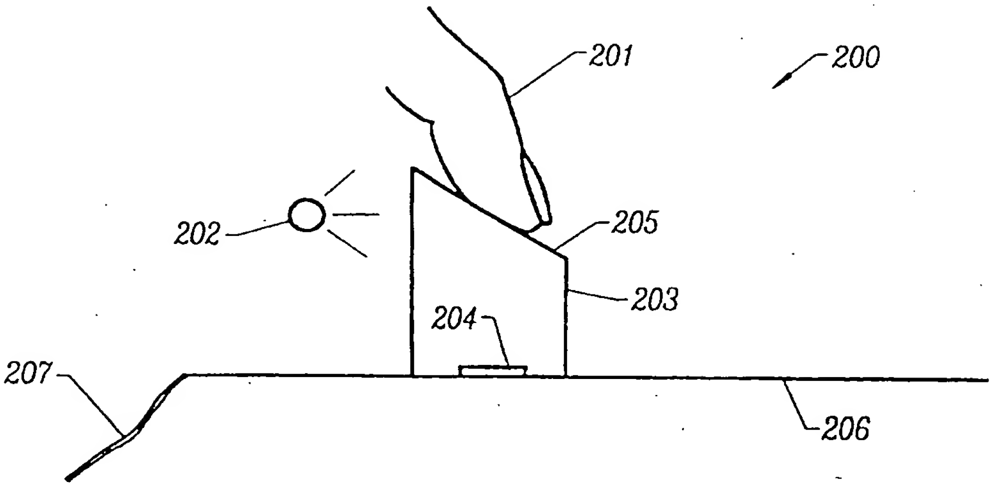


FIG. 2A

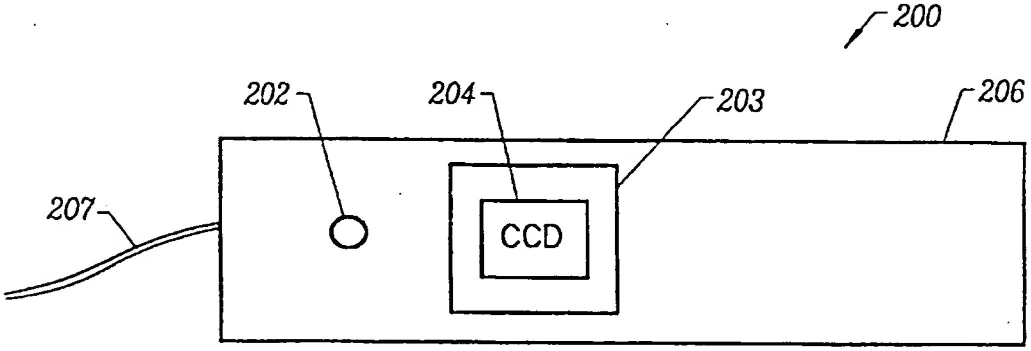


FIG. 2B

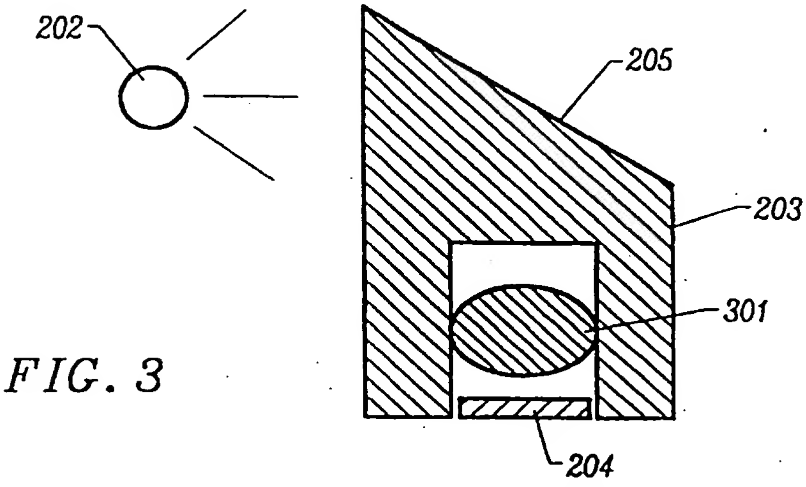


FIG. 3

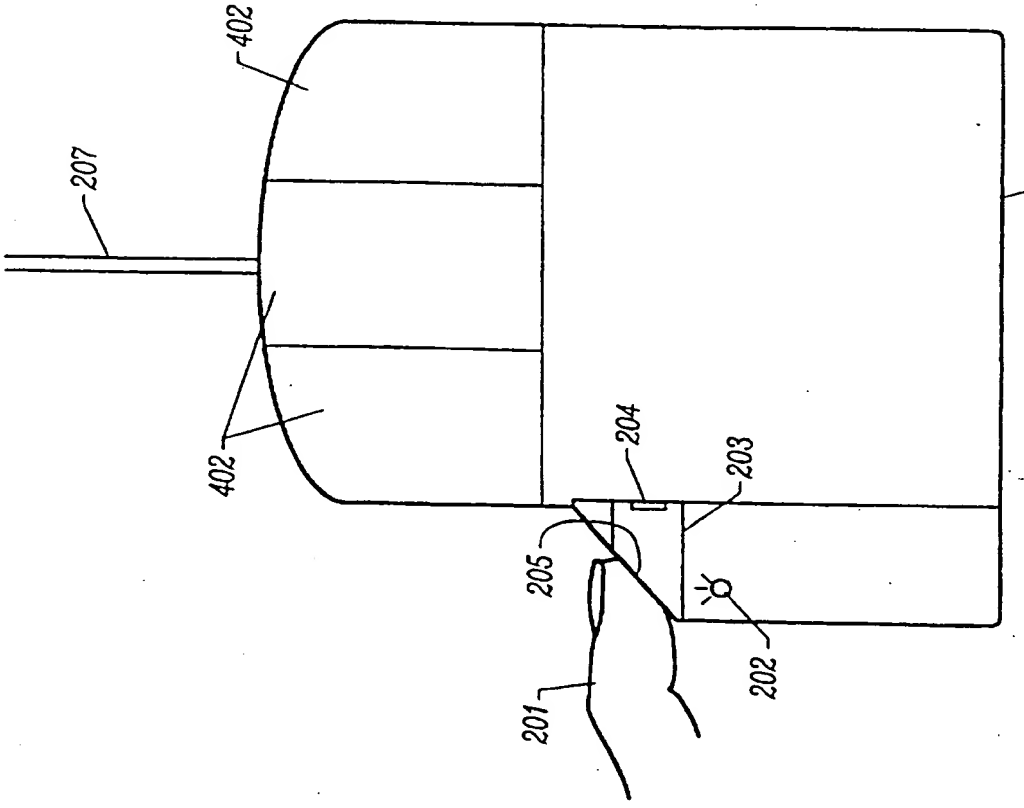

402
207
402
401
204
203
205
202
201

FIG. 4A

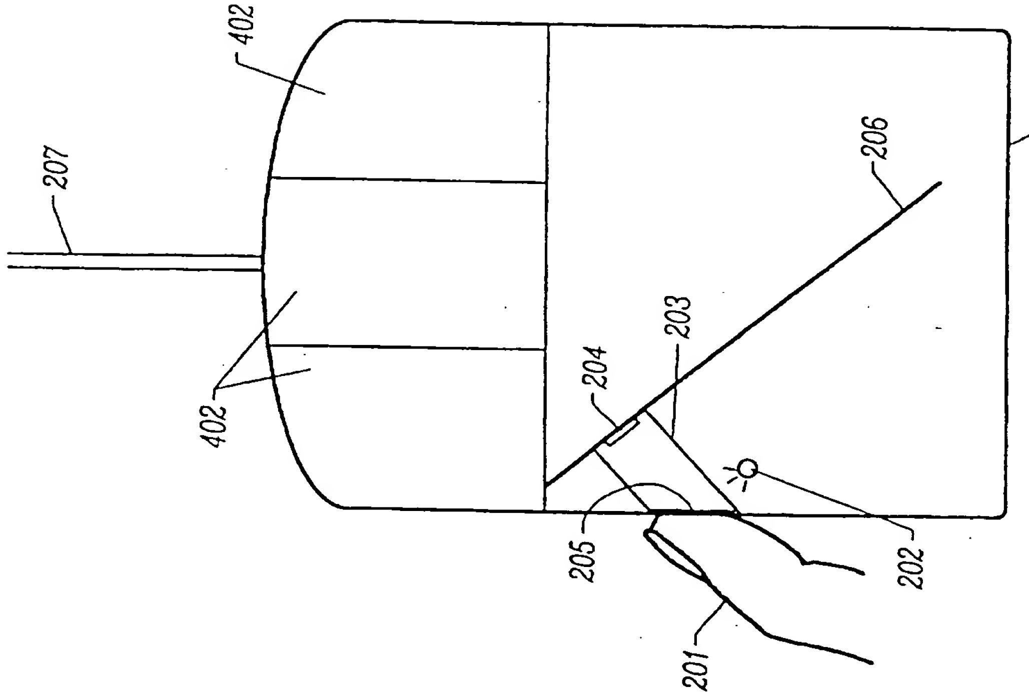

402
207
401
206
203
204
402
205
202
201

FIG. 4B

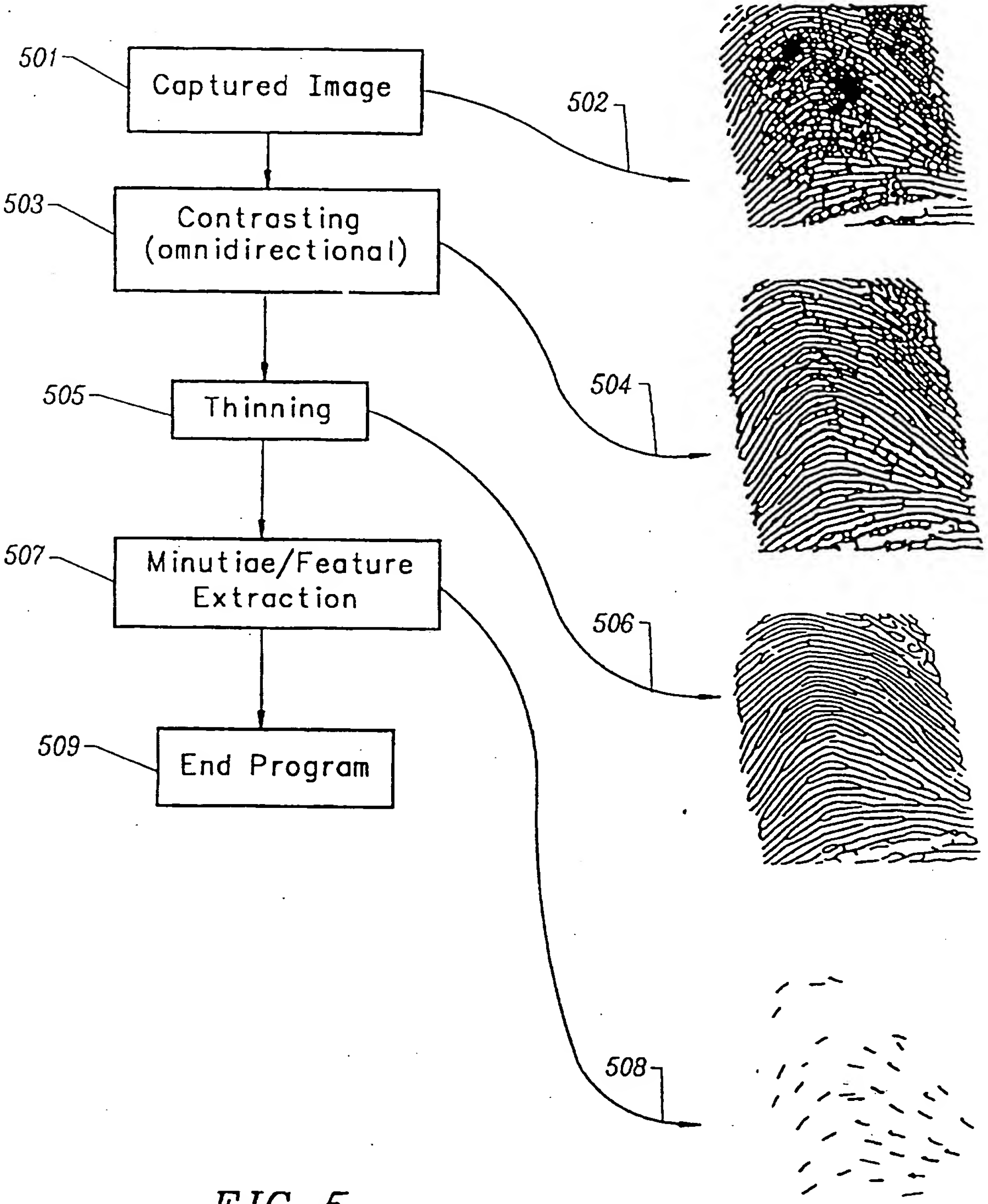


FIG. 5
(PRIORART)

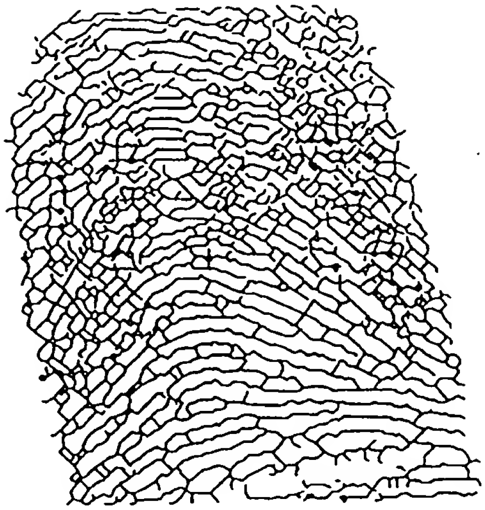


FIG. 6

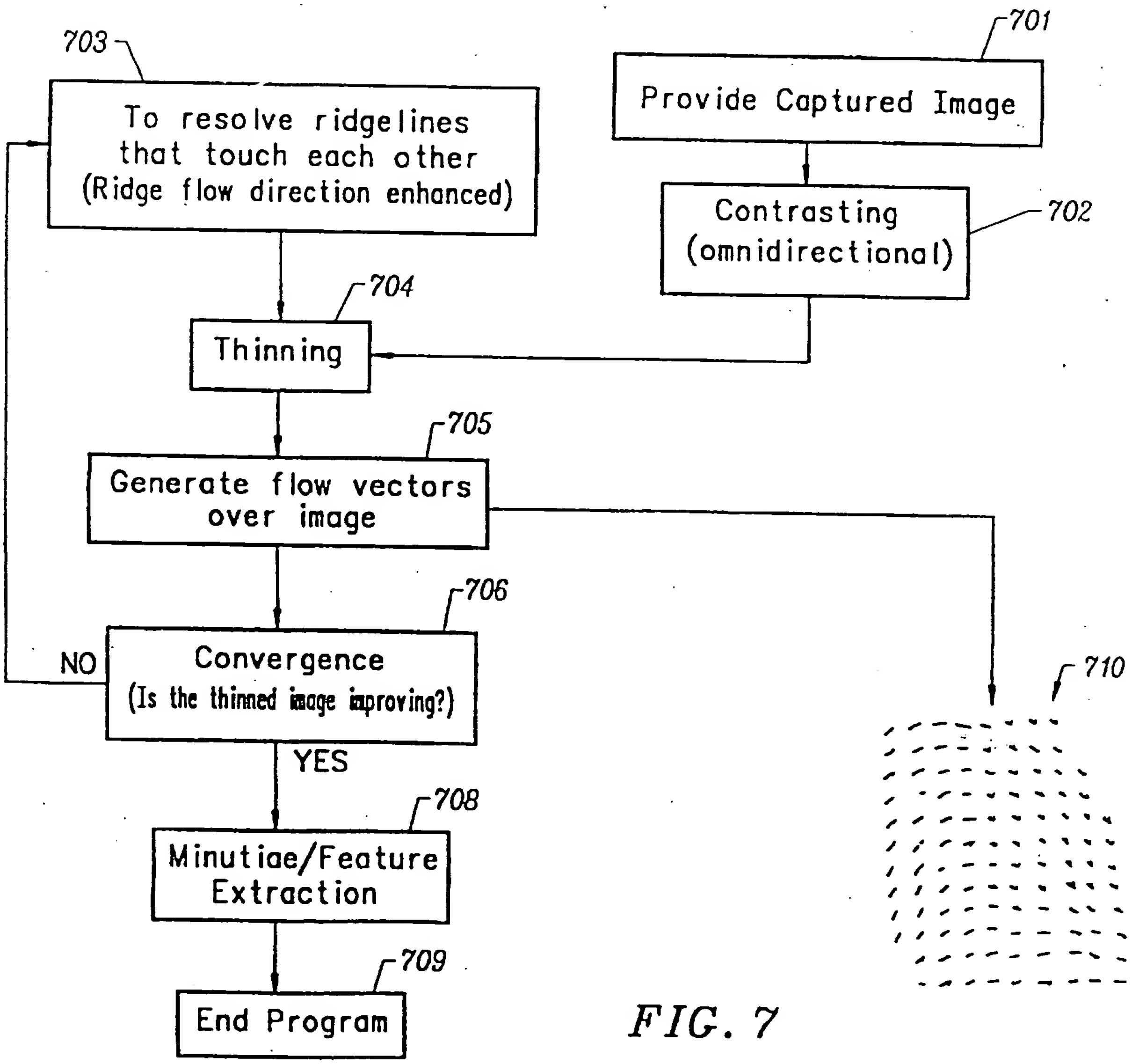

701
Provide Captured Image
702
Contrasting (omnidirectional)
703
To resolve ridgelines that touch each other (Ridge flow direction enhanced)
704
Thinning
705
Generate flow vectors over image
706
Convergence (Is the thinned image improving?)
NO
YES
708
Minutiae/Feature Extraction
709
End Program
710

FIG. 7

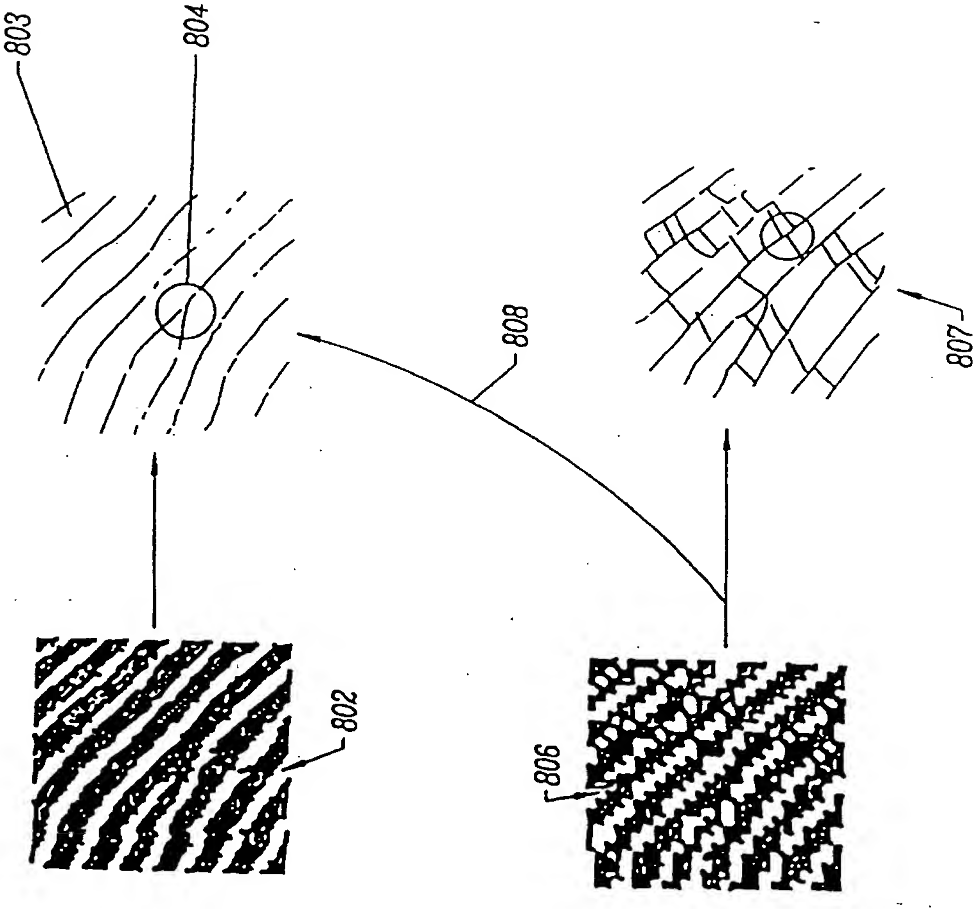


FIG. 8